U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, NY 10007

February 2, 2018

By ECF

The Honorable Jesse M. Furman
United States District Judge
Southern District of New York
40 Foley Square
New York, New York 10007

Re: United States v. Zhengquan Zhang,
17 Cr. 560 (JMF)

Dear Judge Furman:

The Government respectfully submits this motion, pursuant to Federal Rule of Criminal Procedure 16(d)(1) and Title 18, United States Code, Section 1835(a), for entry of the attached proposed protective order governing the disclosure of trade secrets to the defense (the "Revised Proposed Protective Order").

BACKGROUND

A. Offense Conduct

Firm-1 is a global financial services firm headquartered in New York, New York, that engages in the trading of publicly traded securities and other financial products. Firm-1 uses proprietary algorithmic trading models to help it predict market movements and make trading decisions (the "Trading Models"). In addition, Firm-1 uses proprietary trading platforms to create, submit, and execute orders on exchanges and market centers (the "Trading Platforms"). (Indictment ¶ 1).

These Trading Models and Trading Platforms contribute substantially to Firm-1's market share and profits. Because of the competitive advantages and economic value that Firm-1 derived from these assets, Firm-1 has put in place substantial measures designed to protect the computer source code that comprised the Trading Models and Trading Platforms from disclosure to a competitor or to the public. These measures include the use of encryption keys to restrict employee access to the data, restrictions on the ability to download data to storage devices, and employee confidentiality agreements. (Indictment ¶ 4).

Firm-1 employed defendant Zhengquan Zhang in technical roles; he was initially based in the greater New York City area and was later based in Firm-1's San Jose, California office. (Indictment ¶ 2). From December 2016 through March 2017, Zhang orchestrated a scheme to steal from Firm-1 both proprietary data, including various Trading Models and Trading Platforms, as well as confidential data associated with other Firm-1 employees, including email data. In furtherance of this scheme, Zhang purposely circumvented efforts by Firm-1 to protect its data from theft, including through the use of network infrastructure located in this District and elsewhere. (Indictment ¶ 3).

For example, Zhang installed on Firm-1's system computer code designed to look for encryption keys to gain access to encrypted portions of the Trading Models. Zhang also modified an application on Firm-1's system to steal the usernames and passwords of other Firm-1 employees to gain access to their email data. Zhang used an area of Firm-1's computer system to store millions of files of data, including unencrypted portions of the source code of the Trading Models and email data for other Firm-1 employees, to which Firm-1 had not granted Zhang access. Zhang sent data, including Trading Models, Trading Platforms, and email data for other Firm-1 employees, from Firm-1's system to an external third-party software development site. (Indictment ¶ 5). Zhang installed on Firm-1's system computer code designed to send the data through a Firm-1 backup server located in this District. (Indictment ¶ 6).

B. Indictment

On September 13, 2017, a grand jury sitting in this District returned indictment 17 Cr. 560 (JMF), which charges Zhang in four counts. Count One charges Zhang with wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2. Count Two charges Zhang with computer fraud, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B), and 2. Count Three charges Zhang with aggravated identity theft, in violation of Title 18, United States Code, Sections 1028A(a)(1), (b), (c)(4), (c)(5), and 2. Count Four charges Zhang with theft of trade secrets, in violation of Title 18, United States Code, Sections 1832 and 2.

C. Discovery[1]

In the course of its investigation, the Government has obtained data from the following sources that it believes contain Firm-1's trade secrets:

- Snapshots of Zhang's directory on Firm-1's system. As alleged in the Indictment, Zhang stored millions of files of data, including source code for the Trading Platforms,

[1] On September 21, 2017, the defense stipulated to a protective order governing "Confidential Material" other than trade secrets. To date, the Government has made five productions of discovery governed by the Confidential Material protective order. The parties are in the process of negotiating an amendment to the Confidential Material protective order to permit the defendant to have greater direct access to the discovery. The Government anticipates that the parties will be

in this directory. The Government obtained this data in response to a subpoena to Firm-1.

- Data from Gitlab, the third-party software development site. As alleged in the Indictment, Zhang sent data, including Trading Models and Trading Platforms, from Firm-1's system to Gitlab. The Government obtained this data in response to search warrants directed to Gitlab.

- Data from three electronic devices seized from Zhang's residence pursuant to a search warrant for the residence. Zhang subsequently executed a consent to search the contents of the devices. Based on a preliminary review of the data extracted from the devices, it appears that they contain copies of the data described in the two categories above.

Consistent with its representations to the Court at the September 14, 2017 conference, the Government in October 2017 began discussing with defense counsel the production of trade secrets and other proprietary material by inspection at an FBI facility using FBI computer equipment. At defense counsel's request, the Government agreed to make the proprietary material available for inspection at an FBI facility near Zhang's residence in California and agreed that the FBI equipment would be loaded with the defense expert's preferred forensic software (Encase).

On October 27, 2017, the Government emailed defense counsel a proposed protective order governing trade secrets and other proprietary material (the "Initial Proposed Protective Order"). On November 2, 2017, the Government notified defense counsel that the production of proprietary material was available for inspection at the FBI facility in Menlo Park, California, subject to the defense's execution of the Initial Proposed Protective Order.

Over the course of calls and emails in mid-November, defense counsel raised concerns regarding certain provisions of the Initial Proposed Protective Order, which the Government attempted to accommodate. For example:

- Defense counsel objected to a provision prohibiting the defense from bringing electronic devices into the FBI facility because members of the defense team reviewing discovery in the FBI facility might need to be able to speak by phone with members of the defense team outside the facility. The Government agreed that the defense would have access to a landline phone in the FBI facility.

- Defense counsel objected to a search provision; the Government agreed to make explicit that the searches must be "reasonable."

---

able to reach agreement on the amendment, at which time the parties will submit the proposal to the Court for entry.

- In response to a concern raised by defense counsel, the Government agreed to add a provision making clear that the prosecution team would not receive a list of files or data accessed by the defense.

- In response to a concern raised by defense counsel, the Government agreed to provide access to the proprietary material not only to the defense expert, but also the expert's support staff.

- In response to a concern raised by defense counsel, the Government agreed that it would meet and confer in good faith should the defense need additional access to the proprietary material in connection with Firm-1's civil lawsuit against the defendant.

On November 14, 2017, the Government emailed defense counsel a revised proposed protective order (the "Revised Proposed Protective Order").[2] On November 20, 2017, defense counsel objected for the first time to the aspect of the proposals requiring the defense to use FBI computer equipment to review the proprietary material. Defense counsel insisted that the defense expert be permitted to use his own equipment and software.

On December 1, 2017, defense counsel objected for the first time to the aspect of the proposals requiring the defense to review the proprietary material at an FBI facility. Defense counsel insisted that the defense expert be permitted to have a copy of the proprietary material on his own computer equipment (*i.e.*, outside the FBI facility) or, in the alternative, be permitted to use his own equipment and software to review the proprietary material at the FBI facility.

The parties continued their discussions in December and January but have been unable to reach agreement.

ARGUMENT

A. Applicable Law

1. Federal Rule of Criminal Procedure 16

This Court has broad discretion to fashion appropriate protective orders related to discovery and disclosure in criminal cases. *See* Fed. R. Crim. P. 16(d)(1); *United States v. Delia*, 944 F.2d 1010, 1018 (2d Cir. 1991). As the Advisory Committee Notes make clear, the power to enter appropriate protective orders is "necessary" because the Court may be called upon to "[c]ontrol . . . abuses." Advisory Committee Notes to Fed. R. Crim. P. 16(d). The considerations that the Court may take into account include "the safety of witnesses and others," "a particular

[2] With the exception of an updated signature block and the insertion of page numbers, the proposed protective order submitted with this motion for entry by the Court is identical to the Revised Proposed Protective Order emailed to counsel on November 14.

danger [of] perjury or witness intimidation," and "the protection of business enterprises from economic reprisals." *Id.*

2. Economic Espionage Act

Congress enacted the Economic Espionage Act of 1996 (the "EEA") "to prevent economic espionage and to maintain the confidentiality of trade secrets." *United States v. Hsu*, 155 F.3d 189, 202 (3d Cir. 1998). Congress intended the statute to reach "virtually every form of illegal industrial espionage," including not only spying by foreign governments and corporate espionage between two competing companies, but also "the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics.'" *Id.* at 201 (quoting H.R. Rep. No. 104-788, at 5 (1996)). Rather than simply define new criminal offenses, however, Congress created a "comprehensive federal criminal statute" intended to "better facilitate the investigation and prosecution of th[e] crime" and thereby "serve as a powerful deterrent." H.R. Rep. No. 104-788, at 7.

Of course, trade secrets derive their economic value from not being known competitors or the public. *See* 18 U.S.C. § 1839(3) (defining "trade secret"). Thus, any public disclosure of a trade secret poses a substantial risk that the trade secret's value to its owner will be significantly diminished, if not destroyed outright. As part of the EEA's comprehensive design, Congress sought to prevent the public disclosure of trade secrets at issue in criminal prosecutions for theft of trade secrets. Thus, Congress enacted a provision explicitly mandating that trial courts "*shall* enter such orders and take other action as may be necessary and appropriate *to preserve the confidentiality of trade secrets*, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835(a) (emphasis added). Section 1835 was enacted "to preserve the confidentiality of alleged proprietary economic information during legal proceedings under the Act consistent with existing rules of criminal procedure and evidence, and other applicable laws." S. Rep. No. 104-359, at 17 (1996). Congress went even further to protect the rights of trade secret owners in the context of criminal discovery when it supplemented Section 1835 in the Defend Trade Secrets Act of 2016. Congress expressly provided that a court "may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential." 18 U.S.C. § 1835(b).

Congress enacted Section 1835 to advance two compelling interests. First, the provision was designed to "'preserve the confidential nature of the information and, hence, its value.'" *United States v. Ye*, 436 F.3d 1117, 1121 (9th Cir. 2006) (quoting H.R. Rep. No. 104-788, at 13); *cf. In re Iowa Freedom of Information Council*, 724 F.2d 658, 662 (8th Cir. 1983) ("Trade secrets are a peculiar kind of property. Their only value consists in their being kept private. If they are disclosed or revealed, they are destroyed."). Second, Congress sought to "encourage[] enforcement actions by protecting owners who might otherwise 'be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying

their worth.'" *Hsu*, 155 F.3d at 197 (quoting H.R. Rep. No. 104-788, at 13); *see also United States v. Yang*, 281 F.3d 534, 543 (6th Cir. 2002) (recognizing that "the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets," including with "the assistance of people willing to cooperate to catch and convict thieves of trade secrets"). Thus, Section 1835 "represent[s] a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *Hsu*, 155 F.3d at 197.

As Section 1835 and the EEA's legislative history make clear, the protection of the confidentiality of a victim's trade secrets is such an overriding interest as to warrant limits on disclosure and other protective measures as appropriate. *See United States v. Roberts*, 08 Cr. 175, 2010 WL 1010000, at *5 (E.D. Tenn. Mar. 17, 2010) ("A certain absurdity exists in requiring [the victim] to publicly disclose the trade secrets at issue in a prosecution of the alleged theft and disclosure of those same trade secrets."). Not only do victims have a strong interest in not being re-victimized when their trade secrets are disclosed to the public and their competitors, but the Government has an interest in effective criminal enforcement under the EEA—one that encourages, rather than discourages, victims to come forward and report offenses.

B. Discussion

Disclosure of Firm-1's trade secrets to the public or to competitors would substantially harm (if not completely destroy) the value of that intellectual property. Public disclosure would also impede the Government's ability to effectively enforce the EEA, because other victims of theft of trade secrets would be discouraged from cooperating in the investigation and prosecution of such crimes. These harms would accrue whether the public disclosure were intentional or inadvertent. The Court should enter the Revised Proposed Protective Order because it is tailored to address these compelling interests while still preserving the defense's ability to inspect and review the trade secrets in preparing to defend the case.

The Revised Proposed Protective Order governs "Proprietary Material," which is defined as "[d]iscovery material . . . that contains and/or reflects Proprietary Information belonging to the defendant's former employer (the 'Victim Company'), including but not limited to information and data that constitutes suspected trade secrets, confidential and proprietary information, and/or contraband contained therein—whether in paper or electronic form." (Revised Proposed Protective Order ¶ 1).[3] Based on the discussions to date, the Government understands the defense's concerns to center on the following provision of the Revised Proposed Protective Order:

[3] The "Proprietary Material" protected by the Revised Proposed Protective Order is not strictly limited to the trade secret data itself. This is because the Government is still reviewing the Proprietary Material to ensure that other data included within the definition of "Proprietary Material"—such as the email data for other Firm-1 employees that the defendant accessed and sent from Firm-1's system to an external website (Indictment ¶ 5) as well as computer code and other data that the defendant edited—does not itself incorporate relevant trade secret data. The

> 2. The Government shall make Proprietary Material available to the defense at the Federal Bureau of Investigation's Silicon Valley Regional Computer Forensics Laboratory, located in Menlo Park, California (the "Facility"), with the following conditions:
>
> a. The materials containing or reflecting Proprietary Material will be made available for inspection by the Government to the defense on a secured computer in a secure room without Internet or network access to other computers and devices. The Government will make available Encase software for the defense's use in examining the Proprietary Material. The defense shall not copy, remove, or otherwise transfer any portion of the Proprietary Material onto any media or device. During visits to the Facility, the defense is permitted to examine and take written notes regarding the Proprietary Material. Such notes shall be deemed "Confidential Material" and shall be treated as such by defense counsel, pursuant to the terms of the proposed Protective Order governing Confidential Material, executed by the defense on September 21, 2017, and any other Protective Order entered in this case. The defense may not bring in any electronic device (including but not limited to computers, tablets, cellular phones, and any electronic media) into the Facility.
>
> b. The Government will keep a log containing the names of individuals inspecting the Proprietary Material. The Government may visually monitor the activities of the persons reviewing the Proprietary Material for the defense, and may conduct reasonable searches of individuals inspecting the Proprietary Material at any point of time during their visit at the Facility, but only to ensure that there is no unauthorized recording, copying, or transmission of the Proprietary Material. The Prosecution Team (to include the New York-based AUSAs and case agents assigned to this matter) will not receive a list of specific files or data accessed by the defense.

(Revised Proposed Protective Order ¶ 2). During the parties' discussions, defense counsel has raised the following objections to this provision that remain unresolved:

First, defense counsel has objected to the proposal to make the Proprietary Material available to the defense only at the FBI Facility. (Revised Proposed Protective Order ¶ 2). In the

---

Government has agreed that based on this review, it will de-designate from the universe of "Proprietary Material" any data that it determines not to be trade secret data. The Government has also agreed that if the defense identifies, during its review of the Proprietary Material, data that it believes is not trade secret data, the Government will meet and confer in good faith regarding designation of the data. Indeed, the Revised Proposed Protective Order includes an express provision permitting the parties to "reach[] a written agreement . . . as to specific documents containing Proprietary Material[]." (Revised Proposed Protective Order ¶ 9).

alternative, assuming the defense is required to inspect the Proprietary Material at the FBI Facility, defense counsel has objected to the proposal to make the Proprietary Material available to the defense only on FBI equipment. (Revised Proposed Protective Order ¶ 2(a)).

In consultation with the Computer Crime & Intellectual Property Section of the Department of Justice, the Government submits that the defense's review of the Proprietary Material at a secure Government facility, using Government equipment that is not connected to the Internet, is the only way to adequately ensure that Firm-1's trade secret data is not lost, stolen, or otherwise distributed—whether intentionally or unintentionally. Even assuming that defense counsel, the defense expert, and the defendant himself all act in good faith and do not intentionally disclose any of the Proprietary Material, use of the defense expert's devices would require copying the Proprietary Material from Government systems to those devices for purposes of the expert's analysis. This copying would create the risk of potential inadvertent disclosure of the data in any number of scenarios, including but not limited to unauthorized access to the devices through system vulnerabilities (such as by password theft or undetected malware being installed on the devices in question); the devices themselves being lost or stolen; or accidental disclosure or transmittal of data. Moreover, it is the Government's understanding that upon completion of his analysis in this case, the defense expert does not intend to purge the Proprietary Material from his devices through a complete reformatting—the only reliable means to ensure that the trade secret data does not remain in the devices—because his devices contain software and data from other cases that he needs to retain. In light of these facts, the defense proposal—to use the defense expert's devices to analyze the Proprietary Material, which data the defense expert would be able to access at his discretion—simply does not adequately protect against the risk of exposure of Firm-1's trade secrets.

Protective orders with provisions similar to the Government's proposal have been entered in other cases involving theft of trade secrets. For example, Judge Koeltl entered a protective order providing that trade secret information would be available for inspection by the defense "only at Government offices." *United States v. Agrawal*, 10 Cr. 417 (JGK) (S.D.N.Y. July 16, 2010) (ECF No. 16); *see also United States v. Liu*, 16 Cr. 79 (E.D. Wis. July 15, 2016) (ECF No. 12) (only at the local U.S. Attorney's Office or local FBI field office).[4] Although these two protective orders did not specify that the trade secret information would be available only on Government equipment, another protective order in a case involving computer source code (as in this case) did so specify. *United States v. Sinovel Wind Group Co.*, 13 Cr. 84 (W.D. Wis. Feb. 5, 2016) (ECF No. 107).

[4] Courts routinely enter protective orders in child pornography cases similarly providing that the offending images be made available for inspection at a Government facility. *See* 18 U.S.C. § 3509(m)(2)(B). Indeed, when the Government asked defense counsel to provide samples of protective orders that the defense considered to be acceptable, defense counsel provided the Government with protective orders from child pornography cases that make the images available for defense inspection at a Government facility.

Second, defense counsel has objected to the provision prohibiting the defense from bringing any electronic device into the FBI Facility. (Revised Proposed Protective Order ¶ 2(a)). The Government included this provision in the Proposed Protective Order because it is a generally applicable rule for all non-FBI visitors to the FBI Facility, including even Assistant U.S. Attorneys. Indeed, the same rule applies to non-FBI visitors to other FBI facilities, including the FBI facility at 26 Federal Plaza. As noted above, to the extent defense counsel's concern is based on the need for members of the defense team reviewing discovery in the FBI Facility to be able to speak by phone with members of the defense team outside the facility, the Government agrees to provide the defense with access to a landline phone in the FBI Facility.

Third, defense counsel has objected to the provision permitting the defense to "take written notes" while examining the Proprietary Material. (Revised Proposed Protective Order ¶ 2(a)). Defense counsel has consistently characterized this provision as limiting the defense to taking notes with pen and paper. To the contrary, the Government agrees that the defense may take written notes (so long as the defense is not simply copying trade secret data) in electronic form, such as in a word processing program. Because the Government maintains that the defense not be permitted to bring electronic devices into the FBI Facility, the defense would have to type those notes on an FBI computer. The Government is willing to work with defense counsel so that the defense can take those notes out of the FBI Facility, such as by printing out a hardcopy or by copying the file containing those notes to a disc.

Fourth, defense counsel has objected to the provision providing that the Government "may visually monitor the activities of the persons reviewing the Proprietary Material for the defense, and may conduct reasonable searches of individuals inspecting the Proprietary Material at any point of time during their visit at the Facility, but only to ensure that there is no unauthorized recording, copying, or transmission of the Proprietary Material." (Revised Proposed Protective Order ¶ 2(b)). The Government proposed this provision to place the defense on notice of the fact that there would be limitations on their expectations of privacy at the FBI Facility (as there are for all non-FBI visitors to FBI secure facilities), and that the FBI would be able to follow up to ensure compliance with the Revised Proposed Protective Order and the generally applicable prohibition on bringing in electronic devices. The Government notes that in another recent case in this District involving the theft of trade secrets, a defendant brought an unauthorized cell phone into the FBI facility at 26 Federal Plaza while he and defense counsel were reviewing trade secret data, which phone was detected when that defendant was seen with a phone charger as he was leaving the facility. Although in that case the defendant does not appear to have transferred any of the trade secret data onto his device, the Government believes that the FBI Facility's restrictions, for which the defense is on notice, should be both implemented and enforced appropriately.

Other protective orders have included similar provisions. *United States v. Sinovel Wind Group Co.*, 13 Cr. 84 (W.D. Wis. Feb. 5, 2016) (ECF No. 107) (theft of trade secrets case). Indeed, a protective order that defense counsel provided to the Government as an example of a protective order that the defense considered to be acceptable provided for even more intensive monitoring

than what the Government proposes here. *United States v. Isabella*, 14 Cr. 207 (D. Colo. Mar. 26, 2015) (ECF No. 32) (child pornography case).[5]

To be clear, the Government contemplates that the "visual monitoring" referenced in the Revised Proposed Protective Order simply involve having an FBI employee spot-check the defense team by physically looking into the room, in order to ensure there are no unauthorized electronic devices being used and that there is no copying of Proprietary Material. As for the search provision, the Government contemplates that search of a member of the defense would only be permitted if there were reasonable cause to believe that he or she had brought an unauthorized electronic device into the FBI Facility, possessed an unauthorized copy of any of the Proprietary Material, or attempted to copy or transfer any of the Proprietary Material.

CONCLUSION

For the foregoing reasons, the Court should enter the Revised Proposed Protective Order.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: /s/
Eun Young Choi / Won S. Shin
Assistant United States Attorneys
Southern District of New York
(212) 637-2187/2226

Cc: Defense Counsel (by ECF)

[5] The stipulated protective order in *Isabella* provided the following procedure for monitoring: "The Spokane FBI Office will install a stand-alone forensics review workstation in an interview room monitored by Closed Circuit (CC) TV. The defense team lodges a standing objection to the camera while forensic review is being conducted. While the non-audio feed will ensure the integrity of FBI space and security of its occupants, the video feed is not of sufficient detail or at an angle that would reveal defense strategy. The Government and its agents expressly agree that no attempt will be made to record any audio from the workstation and that no attempt will be made to observe the defense team's work product or computer monitor screen at any time. The defense expert may review the feed to ensure that their strategy is not being compromised at any time while conducting the forensic review."